UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,795	08/29/2001	Larry Hamid	12-61 US	4658

25319 7590 08/09/2005

FREEDMAN & ASSOCIATES
117 CENTREPOINTE DRIVE
SUITE 350
NEPEAN, ONTARIO, K2G 5X3
CANADA

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/940,795	HAMID, LARRY	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,5 and 7-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5 and 7-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 16 June 2005. Claims 1, 4, 7, 8, 10, and 14 have been amended. Claims 3 and 6 have been canceled. No new claims have been added. Claims 1, 2, 4, 5, and 7-18 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 16 June 2005 have been fully considered but they are not persuasive.

In reference to the rejection of Claims 1, 2, and 4 under 35 U.S.C. 102(e) as anticipated by Matyas, Jr. et al, US Patent 6697947, and the rejection of Claim 5 under 35 U.S.C. 103(a) as unpatentable over Matyas in view of Schneier, *Applied Cryptography*, and specifically in reference to amended independent Claim 1, Applicant argues that Matyas does not disclose the added limitation of different subsets having different access privileges. This argument is rendered moot in view of the new ground(s) of rejection set forth below. In reference to the limitation previously recited in canceled dependent Claim 6 and now incorporated into Claim 1, Applicant further argues that Schneier does not disclose different subsets having different access privileges and only teaches reconstruction of a same secret by different persons where different numbers of persons belonging to different groups are able to reconstruct the secret. The Examiner respectfully disagrees, noting that a cited portion of Schneier

does indeed show different subsets of persons having different privileges (see Schneier, page 73, "Secret-Sharing Schemes with Prevention").

3. Applicant's arguments with respect to claims 7-18 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 2, 4, 5, and 7-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the subset" in lines 13 and 14 of the claim. It is unclear to which of the subsets in the plurality of predetermined subsets (lines 7-8) this is intended to refer. This renders the claim indefinite. Claim 2 similarly recites the limitation "the subset" in line 2 of the claim.

Further, Claims 1, 7, 10, and 14 each recite the limitation "wherein some of the subsets of the plurality of predetermined subsets". The use of the term "some" is generally vague, as it does not provide a specific numerical range or a clear basis for comparison. This renders the claims indefinite.

Claims not specifically referred to above are rejected due to dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas, Jr. et al, US Patent 6697947, in view of Schneier, *Applied Cryptography*.

In reference to Claim 1, Matyas discloses a method including storing biometric data of each of M designated persons (column 9, lines 5-11 and 55-60), capturing biometric information of each of N persons and providing biometric data corresponding to the captured biometric information where N<M (column 1, lines 43-48, where authentication messages include biometric data; column 9, lines 16-20; column 9, lines 66-column 10, line 4), comparing the captured biometric data with the stored biometric data (column 9, lines 20-24; column 10, lines 4-6), and determining access privileges if the results of the comparison authenticate the N users as a subset of the members of the group of M persons (column 9, lines 11-14 and 24-28 where n=M and k=N; column 10, lines 9-13). Matyas further discloses the use of biometrics to authenticate a threshold scheme for key sharing (see column 15, lines 25-46). However, Matyas does not explicitly disclose that some of the subsets of a plurality of predetermined subsets have different access privileges.

Schneier discloses that secret sharing threshold schemes can be used to model any sharing scheme (see page 72, first paragraph). Schneier further discloses that different subsets can have different access privileges (page 73, "Secret-Sharing Schemes with Prevention"; see page 71, section 3.7, third paragraph; page 72, first paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Matyas to include differing access privileges for different subsets, in order to increase the versatility of the system (see Schneier, page 72, first sentence).

In reference to Claim 2, Matyas further discloses that the subset is a set of X persons, where X is at least equal to N (column 9, lines 11-14 where X=N=k).

In reference to Claim 4, Matyas further discloses that each subset is a different combination (column 9, lines 11-14, where any k of the users must present valid biometric samples to create a valid verification). Schneier also discloses that each subset can be a different combination of users (page 72, first paragraph; page 73 "Secret-Sharing Schemes with Prevention").

In reference to Claim 5, Schneier discloses that secret sharing threshold schemes can be used to model any sharing scheme, such as different numbers of people in different groups (see page 72, first paragraph).

8. Claims 7-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Schneier and applicant admitted prior art.

In reference to Claim 7, Matyas discloses a method including providing each of M designated persons with a device operable to capture biometric information (see column 7, lines 39-57), storing biometric data of each of the M designated persons (column 9, lines 5-11 and 55-60), capturing biometric information of each of N persons and providing biometric data corresponding to the captured biometric information where N<M (column 1, lines 43-48, where authentication messages include biometric data; column 9, lines 16-20; column 9, lines 66-column 10, line 4), comparing the captured biometric data with the stored biometric data and transmitting an authorization signal if the result of the comparison authenticates the user (column 9, lines 20-24; column 10, lines 4-9), and determining access privileges if the authorization signals authenticate at least N users as a subset of the members of the group of M persons (column 9, lines 11-14 and 24-28 where n=M and k=N; column 10, lines 9-13). Matyas further discloses the use of biometrics to authenticate a threshold scheme for key sharing (see column 15, lines 25-46). However, Matyas does not explicitly disclose that some of the subsets of a plurality of predetermined subsets have different access privileges.

Schneier discloses that secret sharing threshold schemes can be used to model any sharing scheme (see page 72, first paragraph). Schneier further discloses that different subsets can have different access privileges (page 73, "Secret-Sharing Schemes with Prevention"; see page 71, section 3.7, third paragraph; page 72, first paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Matyas to include differing access privileges for different subsets, in order to increase the versatility of the system

(see Schneier, page 72, first sentence). Further, although Matyas does disclose that the computer system used may be handheld and may be embodied in other devices (column 7, lines 29-38), neither Matyas nor Schneier explicitly disclose the use of a portable biometric device.

Applicant admits as prior art a portable fingerprint recognition and transmission device (page 4, paragraph 0012 of Applicant's specification). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Matyas by including the use of such a portable biometric device, in order to take advantage of the smaller, lighter, less burdensome, and more portable miniaturized devices (see paragraph 11 of Applicant's specification).

In reference to Claim 8, Matyas discloses that access is denied in absence of at least N of M authorization signals (column 9, lines 29-37; column 10, lines 13-21).

In reference to Claim 9, Matyas discloses that the subset includes at least two persons (see, for example, column 1, lines 43-47, where the method is for "multi-party authentication").

In reference to Claims 10 and 13, Matyas discloses a method including storing biometric data of each of M designated persons (column 9, lines 5-11 and 55-60), capturing biometric information of each of N persons and providing biometric data corresponding to the captured biometric information where N<M (column 1, lines 43-48, where authentication messages include biometric data; column 9, lines 16-20; column 9, lines 66-column 10, line 4), comparing the captured biometric data with the stored

biometric data (column 9, lines 20-24; column 10, lines 4-9), transmitting an authorization signal for each of X (where X=N) comparison results that authenticate the N users as a subset of the members of the group of M persons (column 9, lines 11-14 and 20-28 where n=M and k=N; column 10, lines 6-13), and determining access privileges depending on the authorization signals (column 9, lines 11-14 and 24-28; column 10, lines 9-13). Matyas further discloses the use of biometrics to authenticate a threshold scheme for key sharing (see column 15, lines 25-46). However, Matyas does not explicitly disclose that some of the subsets of a plurality of predetermined subsets have different access privileges.

Schneier discloses that secret sharing threshold schemes can be used to model any sharing scheme (see page 72, first paragraph). Schneier further discloses that different subsets can have different access privileges (page 73, "Secret-Sharing Schemes with Prevention"; see page 71, section 3.7, third paragraph; page 72, first paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Matyas to include differing access privileges for different subsets, in order to increase the versatility of the system (see Schneier, page 72, first sentence). Further, although Matyas does disclose that the computer system used may be handheld and may be embodied in other devices (column 7, lines 29-38), neither Matyas nor Schneier explicitly disclose the use of a portable biometric device.

Applicant admits as prior art a portable fingerprint recognition and transmission device (page 4, paragraph 0012 of Applicant's specification). Therefore, it would have

been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Matyas by including the use of such a portable biometric device, in order to take advantage of the smaller, lighter, less burdensome, and more portable miniaturized devices (see paragraph 11 of Applicant's specification).

In reference to Claims 11 and 12, Matyas further discloses that access privileges include functional limitations (for example, see column 16, lines 42-49, where the biometric data are used to recover a shared key) and can define a time limitation (see column 9, lines 38-53, where the times during which the system can be accessed are limited; see also column 6, lines 19-26, where biometric techniques can be used for various applications including time recording).

In reference to Claim 14, Matyas discloses a system including at least one device (see column 7, lines 39-57) that includes a biometric sensor and an encoder for providing biometric data based on biometric information captured by the biometric sensor (Figure 1, biometric information input device 35), a memory (Figure 1, memory 36) for storing biometric data of at least one of M designated persons (column 9, lines 5-11 and 55-60), and a processor (figure 1, processor 38) for comparing the captured biometric data with stored biometric data and producing an authorization signal if the comparison indicates a match (column 9, lines 20-24; column 10, lines 4-9). Matyas further discloses a port for receiving the authorization signals (column 9, lines 16-20) and a processor for determining access privileges dependent on the authorization signals of a subset of N persons of the group of M persons, where N<M (column 9, lines

11-14 and 24-28 where n=M and k=N; column 10, lines 9-13). Matyas further discloses the use of biometrics to authenticate a threshold scheme for key sharing (see column 15, lines 25-46). However, Matyas does not explicitly disclose that some of the subsets of a plurality of predetermined subsets have different access privileges.

Schneier discloses that secret sharing threshold schemes can be used to model any sharing scheme (see page 72, first paragraph). Schneier further discloses that different subsets can have different access privileges (page 73, "Secret-Sharing Schemes with Prevention"; see page 71, section 3.7, third paragraph; page 72, first paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Matyas to include differing access privileges for different subsets, in order to increase the versatility of the system (see Schneier, page 72, first sentence). Further, although Matyas does disclose that the computer system used may be handheld and may be embodied in other devices (column 7, lines 29-38), neither Matyas nor Schneier explicitly disclose the use of a portable biometric device, nor that the device specifically includes a transmitter.

Applicant admits as prior art a portable fingerprint recognition and transmission device, including a transmitter (page 4, paragraph 0012 of Applicant's specification). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Matyas by including the use of such a portable biometric device, in order to take advantage of the smaller, lighter, less burdensome, and more portable miniaturized devices (see paragraph 11 of Applicant's specification).

In reference to Claim 15, Matyas further discloses that the biometric sensor can be a fingerprint sensor (column 6, lines 13-19).

In reference to Claim 16, Applicant further admits that the portable biometric device includes a wireless transmitter (page 4, paragraph 0012 of Applicant's specification, where a transmitter is infrared or radio).

In reference to Claim 17, Applicant further admits that the portable biometric device is handheld (page 4, paragraph 0012 of Applicant's specification).

9. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Schneier and applicant admitted prior art as applied to claim 17 above, and further in view of Schneider et al, US Patent 5456256.

Matyas as modified above discloses everything as applied to Claim 17 above, and Matyas further discloses the use of a card for storing authentication information (column 11, lines 5-8). However, neither Matyas, Schneier, nor the applicant admitted prior art explicitly disclose that the handheld portable biometric device is a smart card. Schneider discloses an imaging system that can be used for identification, which can be embodied in a smart card (column 24, lines 50-64). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the system of Matyas as modified above, by using a smart card as the portable biometric device, in order to minimize delay and inconvenience (see Schneider, column 1, lines 26-29).

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER